(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平9－297828

(43)公開日　平成9年(1997)11月18日

(51)Int.Cl.⁶	識別記号	庁内整理番号	FI		技術表示箇所
G06K	17/00		G06K	17/00	T
	19/10			19/00	R
	19/06				B
G07F	7/12		G07F	7/08	B

審査請求　有　請求項の数6　FD　（全 6 頁）

(21)出願番号　特願平8－137580

(22)出願日　平成8年(1996)5月8日

(71)出願人　596048536
松本　勉
神奈川県相模原市上鶴間2603－1　サンヴェール町田グランデュール210
(71)出願人　000004640
日本発条株式会社
神奈川県横浜市金沢区福浦３丁目10番地
(72)発明者　松本　勉
神奈川県相模原市上鶴間2603－1　サンヴェール町田グランデュール210
(74)代理人　弁理士　大島　陽一

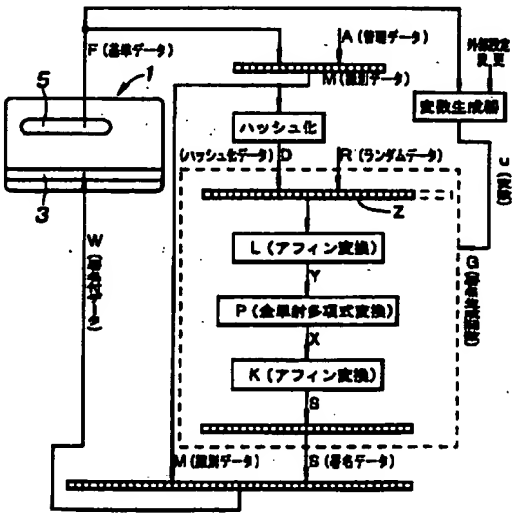
最終頁に続く

(54)【発明の名称】　認証式セキュリティシステム

(57)【要約】

【課題】　カードなどのデータ記録媒体に於いて、データを新たに生成したり、データを改竄することを効果的に防止する。

【解決手段】　基準データを含むデータを、基準データにより生成された変数に応じた方法で変換して署名データを生成し、逆変換して識別データを認証する構成とすることにより、署名生成ルールが基準データ（により生成された変数）により変化することから、媒体（対象物）やそのリーダライタから署名生成ルールの解析を行うことが極めて困難になり、比較的複製されやすい磁気データの偽造及び改竄を著しく困難にすることができる。



1

【特許請求の範囲】

【請求項１】　真正性の判定を必要とする対象物の偽造及び複製を防止するためのセキュリティシステムであって、

書き込み時に個別に設定される基準データに基づく識別データを記憶保持するための識別データ格納領域と、

前記識別データを認証するための署名データを記憶保持するための署名データ格納領域とを有し、

前記署名データが、前記識別データまたは前記基準データを含むデータを、前記識別データまたは前記基準データにより生成された変数に応じた方法で変換してなり、

真正性の判定が、前記署名データを前記識別データまたは前記基準データにより生成された変数に応じた方法で逆変換してなるデータによる前記識別データの認証結果に基づき行われることを特徴とする認証式セキュリティシステム。

【請求項２】　対象物に設けられ、かつ機械により読み取り可能であるが、物理的に無作為に生成されているために人為的に同一なものを製作することが困難な基準領域に記録されたデータの読み取り結果を前記基準データとすることを特徴とする請求項１に記載の認証式セキュリティシステム。

【請求項３】　真正性の判定が、該判定時に前記基準領域から読み取ったデータと、前記識別データまたは前記署名データに含まれる前記基準データとの照合結果と、

前記署名データを前記識別データまたは前記基準データにより生成された変数に応じた方法で逆変換してなるデータによる前記識別データの認証結果とに基づき行われることを特徴とする請求項１若しくは請求項２に記載の認証式セキュリティシステム。

【請求項４】　前記識別データが、当該対象物を管理するための管理データと前記基準データとを併せたデータからなることを特徴とする請求項１乃至請求項３のいずれかに記載の認証式セキュリティシステム。

【請求項５】　前記署名データが、前記識別データをデータ圧縮した圧縮識別データに基づいて生成されていることを特徴とする請求項１乃至請求項４のいずれかに記載の認証式セキュリティシステム。

【請求項６】　前記基準領域が、紙または樹脂中に磁性体繊維を無作為に配置したものからなることを特徴とする請求項２乃至請求項５のいずれかに記載の認証式セキュリティシステム。

【発明の詳細な説明】

【０００１】

【発明が属する技術分野】本発明は、例えば、プリペイドカード、クレジットカード、ＩＤカードなどの真正性の判定を要する対象物の偽造及び複製を防止するためのセキュリティシステムに関する。

【０００２】

2

【従来の技術】また、従来のセキュリティーシステムの１つの手法として、署名生成ルールを用いて元のデータから署名データを生成し、署名検査ルールを用いて上記署名データを検査して元のデータの真正性を確認する認証システムが知られている。このシステムによれば、署名検査ルールを知る者が、署名データを検査して元のデータの真正性を確認できる。また、署名生成ルールを知る者のみが、自らの署名付きデータを新たに生成したり、当該データを改変することができる。このシステムにより効果的にデータの真正性を判定することができるため、対象物にデータの記録媒体をシール化するなどして添付し、その真正性を保証する仕組みも試みられている。

【０００３】しかしながら、このシステムにあっては、不正な目的で署名付きデータと元のデータとのサンプルを複数個入手するなどして、データの解析を行い、署名生成ルールを解読して署名付きデータを新たに生成したり、当該データを改竄することも不可能ではない。

【０００４】

【発明が解決しようとする課題】このような従来技術の問題に鑑み、本発明の主な目的は、対象物の偽造及び複製を効果的に防止し、安全性の高いセキュリティシステムを提供することにある。

【０００５】

【課題を解決するための手段】上記の目的は本発明によれば、真正性の判定を必要とする対象物の偽造及び複製を防止するためのセキュリティシステムであって、書き込み時に個別に設定される基準データに基づく識別データを記憶保持するための識別データ格納領域と、前記識別データを認証するための署名データを記憶保持するための署名データ格納領域とを有し、前記署名データが、前記識別データまたは前記基準データを含むデータを、前記識別データまたは前記基準データにより生成された変数に応じた方法で変換してなり、真正性の判定が、前記署名データを前記識別データまたは前記基準データにより生成された変数に応じた方法で逆変換してなるデータによる前記識別データの認証結果に基づき行われることを特徴とする認証式セキュリティシステムを提供することにより達成される。

【０００６】このように、人為的に同一なものを製作することが困難な基準領域から所定の機械によって読み取って得られるか任意に選択される基準データ、またはそれによって照合されるべき識別データに基づき、かつ基準データから生成された変数に応じた方式で生成された署名データによってのみ識別データ格納領域に記憶保持された識別データの真正性を確認できるようにしたため、例えば複数のサンプルを用いても署名生成ルールが各々異なることからこれを解析することは著しく困難であり、かつこの各々の署名生成ルールを知らずに、署名付きデータを新たに生成したり、当該データを改竄する

ことも極めて困難になる。

【0007】特に、判定時に基準領域から読み取ったデータと、識別データまたは署名データに含まれる基準データとの照合結果と、上記認証結果とに基づき真正性の判定を行うことにより、署名付きデータのみを単にデッドコピーしても他の対象物では判定時に基準領域から読み取ったデータと基準データとの一致度が低いことからその真正性は否定され、即ち他の対象物への不正な適用をも効果的に防止することができる。

【0008】また、対象物を管理するために必要な情報であるところの管理データを基準データと合わせて識別データとすることにより、この管理データを当該対象物や当該署名生成者についての情報などと別途照合すれば、署名付きデータを新たに生成したり、当該データを改竄することを一層効果的に防止することができる。

【0009】更に、署名データが識別データをデータ圧縮した圧縮識別データに基づいて生成されているものとすることにより、処理に必要なビット長を抑制することができ、署名検査に要する時間を短縮することができる。

【0010】基準領域として、紙又は樹脂中に磁性体繊維を無作為に配置したものや、紙の漉きむらを利用したり、シート材の表面粗さなど、人為的に複製することが困難で、しかも所定の機械では再現性良く検出し得るものであれば、任意のものを用いることができる。そのような例としては、特開平6－168363号、特開昭52－33444号、特表昭57－500851号の各公報に開示されたものなどがある。

【0011】

【発明の実施の形態】以下、本発明の好適実施形態を添付の図面について詳しく説明する。

【0012】図1は、本発明が適用されたプリペイドカードを示す。このカード1はポリエステル製のシート2からなり、このカードには、発行者、券種やカードの使途を特定する管理データと後記する基準データとを合わせて識別データとして格納するための識別データ格納領域を含む磁気ストライプ3と、度数の消費に伴い穿孔されるべき穿孔領域4と、磁性体繊維をベースシート2の樹脂中に無作為に分散してなる基準領域5とが設けられている。磁気ストライプ3には、さらに後記する署名データ格納領域が含まれている。

【0013】図2は、本発明が適用されたカードリーダを示す。カードリーダ10は、カードをスロット11内に取り込み、データ読み取り後にカードを排出するためのモータ駆動されたローラを含むカード搬送ユニット12が内蔵されている。スロット11に沿って、磁気ストライプ3を読み取るための磁気ヘッド13及び基準領域5を読み取るための誘導式磁気ヘッド14が設けられている。尚、符号15は、度数の消費を示すべくカードの穿孔領域4に順次穿孔を行ったり、また必要に応じて使用済みの基準領域5を破壊するべく該領域に穿孔を行うための穿孔ユニットを示す。

【0014】次に、図3について、カード1の署名データ生成手順、即ちカードの作成手順を説明する。まず、カードリーダ側に設定された読み取り軌跡に沿って、基準領域5から信号を機械的に読み取り、それを基準データFとして管理データAと組み合わせ、これを4つの64ビットデータブロックm_1～m_4からなる識別データMとして、磁気ストライプ3の識別データ格納領域に書き込む。次に、識別データMに対して、図4に示されるようなハッシュ化過程を行う。即ち、まずデータブロックm_1を、固定された64ビットデータブロックh_0、h_0'に組み合わせて2つの64ビットデータブロックh_1、h_1'を得る。次に、データブロックm_2を、それらの64ビットデータブロックh_1、h_1'に組み合わせて2つの64ビットデータブロックh_2、h_2'を得る。このようなステップを4回繰り返し、2つの64ビットデータブロックh_4、h_4'を得る。最終的に得られるハッシュ化データDは128ビットのデータ長を有する。

【0015】このハッシュ化データDに、図3に示されるように、所定のランダムデータRを組み合わせて、書き込む署名データ長に合わせた、例えば100ビットの入力データZとする。この入力データZに対して、アフィン変換L、全単射多項式変換P、アフィン変換Kを順次行い（Z→Y→X→S）、すなわち署名生成関数Gによる演算によって、最終的な署名データSを得て、それを前記した識別データMと共に磁気ストライプ3の各々の格納領域に書き込む。このようにして磁気ストライプ3に書き込むデータ全体を署名付データWと呼ぶものとする。その際、署名データ格納領域及び識別データ格納領域は、互いに独立に配置されたものでも良いが、図示されていない任意の暗号化手法により暗号化したデータとすることもできる。

【0016】ここで、全単射多項式変換Pは、有限体上の任意の元Yをある特定の元Xに変換するもので、署名生成ルールの解析の困難さは、有限体上の多変数連立方程式を解くことの難しさに基づいている。更に、後記する署名検査関数Vから署名生成関数Gが容易に推測されないように、変換の前後にアフィン変換を行う。また、ハッシュ化過程におけるh_0、h_0'に各々任意の定数を選択することが可能である。

【0017】また、署名生成関数Gにおけるアフィン変換L、K、全単射多項式変換Pにおいても各々任意の定数を選択することが可能であるが、本願に於ては各定数を基準データFから生成された固有の変数uに応じて設定または変更し得るようになっている。これは例えば変数uと各定数とのテーブルを参照しても良いし、別途関数などを用いて変数uから各定数を生成するようにしても良い。実際には例えば変数uに応じて全単射多項式変換Pの変換アルゴリズムを変更する構成としても良い。

このようにして多様な認証システムを形成することができ、署名生成ルールを推定し難いものとしている。更に、署名生成時にランダムデータRを連接していることにより、一層効果的に署名生成ルールを推定し難いものとしている。

【００１８】このカード１を使用する際には、先ず、図５に示されるように、磁気ストライプ３から得られた署名付データW′のうちの識別データM′を基準データF′と管理データA′とに分離する。ここで、この基準データF′を、誘導式磁気ヘッド１４によって基準領域から得られる基準データF″と比較して、カードの真正性及びデータの偽造及び改竄の有無をチェックする。そして、その比較結果が適正であると確認されたら、識別データM′に対して、前記と同様にハッシュ化処理を行い、ハッシュ化データD′を得る。同時に署名付データW′のうちの署名データS′を多変数多項式タプルQによる逆変換（前記Z→Y→X→Sの逆変換過程に相当）、即ち署名検査関数Vによる演算によって逆変換する。このとき、基準データF′から上記同様にして変数u′を生成し、多変数多項式タプルQに用いる定数、または逆変換アルゴリズムを求める。この多変数多項式タプルQによる逆変換で求められたデータをハッシュ化データD″とランダムデータR′とに分離する。このようにして得られた２つのハッシュ化データD′とD″とを比較することにより、署名検査を行い、データの偽造及び改竄の有無をチェックする。そして、その比較結果が適正であることが確認された場合、つまりカードの真正性が確認された場合のみ、判定器から適性信号を出力し、アプリケーションに応じた所定のサービスを提供する。また、これに加えて、管理データA′が、予め記憶されている図示されない管理データAと同一であることが確認された場合、適性信号を出力するようにしても良い。

【００１９】ここで、上記したように同一の基準領域を複製することは実質的に不可能であることから、カードのデッドコピーは防止できる。また、誘導式磁気ヘッド１４によって基準領域から得られる基準データF″はカードの搬送、停止位置の誤差、汚損度、磁気の経年劣化などの様々な要因により読み出す度にその値が異なる。従って、実際には所定値以上の一致度となったか否かによりカードの真正性をチェックする。例えば、不正使用の目的で磁気データとしての識別データM′から基準データF′を抽出し、基準領域５から基準データF″を読み出し、両者を比較して両者間の関係を解明しようとしても、上記した理由で基準データF″が読み出す度に変化することから、複数のサンプルを用いてもその関係を特定することができず、不正に任意の基準領域を有するカードを作成し、その基準データに対応させて識別データM′を作ることも極めて困難となる。しかも、その識別データを基に署名データを作ることは上記したように極めて困難であることから、データの改竄も極めて困難である。従って、カード（対象物）のデッドコピー、偽造（複製）、データ改竄のいずれも極めて困難であることから実質的に対象物に対する不正行為が不可能となる。

【００２０】尚、上記実施形態では磁性体繊維をベースシート２の樹脂中に無作為に分散して基準領域５を形成したが、例えば単に変数ｕを記録するためのバーコードなどで形成しても良く、また記録／読み取りの周期の短い用途であれば、対象物側に基準領域を設けず、リーダライタ側に基準データを設定しておき、これを定期または不定期に変更するようにしても良い。

【００２１】また、図３及び図５に示すように、上記変換の各定数の変数ｕに対応する設定、例えば変数ｕと各定数とのテーブルまたは変数ｕから各定数を生成する関数を外部から設定変更するようにしても良い。これは、変数ｕに応じて全単射多項式変換Ｐの変換アルゴリズムを変更する場合も同様である。

【００２２】加えて、上記実施形態では対象物を例えば情報記憶カードまたはＩＤカードとしたが、固有の価値が証明された貴金属類、有価証券、部屋や自動車のキーなど、真正なものであることを証明する必要のあるものに任意に適用できることは云うまでもない。

【００２３】

【発明の効果】このように、本発明によれば、比較的少ないビット長の署名データで複雑な認証システムを実現することができる。しかも、署名生成及び署名検査に要する処理時間が増加することもなく、アルゴリズム構築に必要なプログラムやメモリ領域の大きさなど、従来のカードリーダライタに組み込み可能な速度・サイズで動作が可能となる。

【００２４】基準データを含むデータを、基準データにより生成された変数に応じた方法で変換して署名データを生成し、逆変換して識別データを認証する構成とすることにより、署名生成ルールが基準データ（により生成された変数）により変化することから、媒体（対象物）やそのリーダライタから署名生成ルールの解析を行うことが極めて困難になり、比較的複製されやすい磁気データの偽造及び改竄を著しく困難にすることができる。即ち、リーダ（署名検査機）を不正に入手して、それを解析したとしても、有限体上の多変数連立方程式を解くことの困難さに基づき、署名生成ルールを推定することは著しく困難であり、しかもこの署名生成ルールが基準データ毎に（例えば対象物が固有の基準データを有していれば対象物毎に）変わることから、その解析は極めて困難となり、署名付データの生成及び変更も効果的に防止できる。

【００２５】更に、人為的に同一なものを製作することが困難な基準領域から読み取った基準データを用い、真正性の判断時にそのときに読み取った基準データと署名

付きの識別データとの照合をも行うことで、対象物であるカードを不正に複製することも極めて困難となる。同様に複数のカードのサンプルからシステムに対する解析を行うことも困難となる。

【図面の簡単な説明】

【図1】本発明に基づくシステムが適用された対象物の一例としてのプリペイドカードを示す正面図。

【図2】プリペイドカードのためのカードリーダの一例を示すダイヤグラム図。

【図3】本発明に基づくカードの作成手順を示すブロック図。

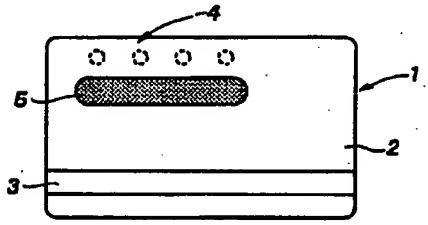
【図4】図3に於けるハッシュ化過程の詳細を示すブロック図。

【図5】本発明に基づくカードの認証及び読み取りの手順を示すブロック図。

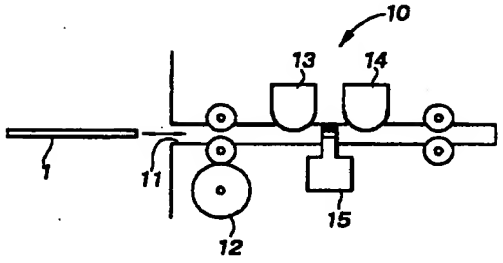
【符号の説明】

1　カード
2　ベースシート
3　磁気ストライプ
4　穿孔領域
5　基準領域
10　カードリーダ
11　スロット
12　カード搬送ユニット
13　磁気ヘッド
14　誘導式磁気ヘッド
15　穿孔ユニット

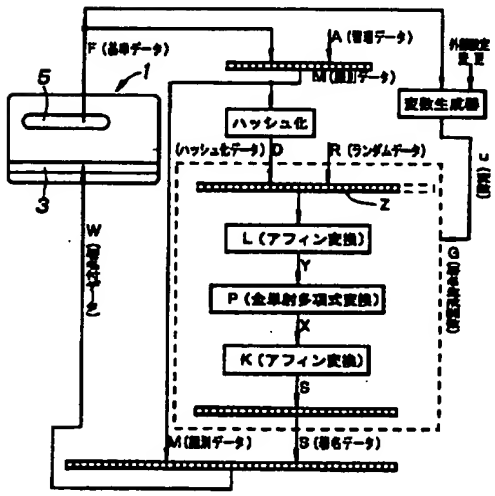
【図1】



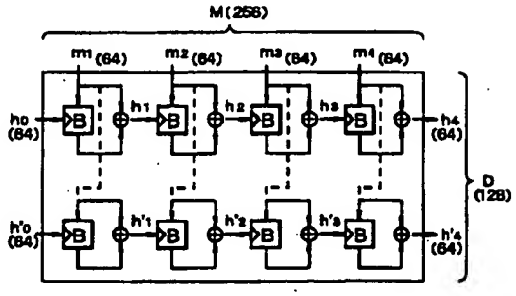
【図2】



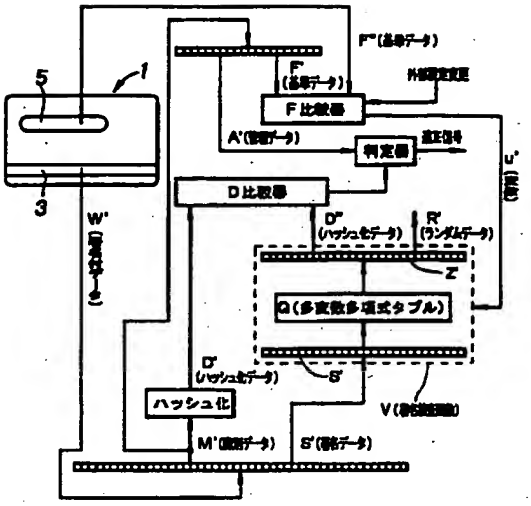
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者　松本　弘之
神奈川県横浜市金沢区福浦３丁目10番地
日本発条株式会社内

(72)発明者　大野　正剛
神奈川県横浜市金沢区福浦３丁目10番地
日本発条株式会社内

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.